DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

CHIEF INFORMATION OFFICER

OCT 16 2009

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES
CHIEF INFORMATION OFFICERS OF THE MILITARY DEPARTMENTS

SUBJECT: Clarifying Guidance Regarding Open Source Software (OSS)

References: See Attachment 1

To effectively achieve its missions, the Department of Defense must develop and update its software-based capabilities faster than ever, to anticipate new threats and respond to continuously changing requirements. The use of Open Source Software (OSS) can provide advantages in this regard. This memorandum provides clarifying guidance on the use of OSS and supersedes the previous DoD CIO memorandum dated May 28, 2003 (reference (a)).

Open Source Software is software for which the human-readable source code is available for use, study, reuse, modification, enhancement, and redistribution by the users of that software. In other words, OSS is software for which the source code is "open."

There are many OSS programs in operational use by the Department today, in both classified and unclassified environments. Unfortunately, there have been misconceptions and misinterpretations of the existing laws, policies and regulations that deal with software and apply to OSS, that have hampered effective DoD use and development of OSS. Attachment 2 contains clarifying guidance to address some of those issues.

I have asked the Director, Enterprise Services & Integration, to work with your staffs and identify other barriers to the effective use of open source software within the Department, so we can continue to increase the benefits from the use of OSS. Additional information to clarify how existing DoD policies relate to open source software will be posted at http://www.defenselink.mil/cio-nii/cio/oss/. Questions concerning this memorandum should be directed to Daniel Risacher, Enterprise Services & Integration, at (703) 602-1098 or email, Daniel.Risacher@osd.mil.

David M. Wennergren
Performing the Duties of the
ASD(NII)/DoD CIO

Attachments:
As stated

ATTACHMENT 1

REFERENCES

(a) DoD Chief Information Officer (CIO) Memorandum, "Open Source Software (OSS) in the Department of Defense (DoD)," May 28, 2003 (superseded)
(b) Title 10, United States Code (USC), Section 2377
(c) Federal Acquisition Regulation (FAR), Sections 2.101, 12.000, 12.101
(d) Defense Federal Acquisition Regulation Supplement (DFARS), Section 227.7203-5
(e) Title 41, United States Code (USC), Section 253a
(f) Federal Acquisition Regulation (FAR), Section 10.001
(g) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
(h) DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004
(i) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987

ATTACHMENT 2

CLARIFYING GUIDANCE REGARDING OPEN SOURCE SOFTWARE (OSS)

1. GENERAL. This attachment provides clarification and additional guidance on the use and development of OSS. It does not change or create new policy, but is intended only to explain the implications and meaning of existing laws, policies and regulations.

2. GUIDANCE

a. In almost all cases, OSS meets the definition of "commercial computer software" and shall be given appropriate statutory preference in accordance with 10 USC 2377 (reference (b)) (see also FAR 2.101(b), 12.000, 12.101 (reference (c)); and DFARS 212.212, and 252.227-7014(a)(1) (reference (d))).

b. Executive agencies, including the Department of Defense, are required to conduct market research when preparing for the procurement of property or services by 41 USC Sec. 253a (reference (e)) (see also FAR 10.001 (reference (f)). Market research for software should include OSS when it may meet mission needs.

(1) There are positive aspects of OSS that should be considered when conducting market research on software for DoD use, such as:

(i) The continuous and broad peer-review enabled by publicly available source code supports software reliability and security efforts through the identification and elimination of defects that might otherwise go unrecognized by a more limited core development team.

(ii) The unrestricted ability to modify software source code enables the Department to respond more rapidly to changing situations, missions, and future threats.

(iii) Reliance on a particular software developer or vendor due to proprietary restrictions may be reduced by the use of OSS, which can be operated and maintained by multiple vendors, thus reducing barriers to entry and exit.

(iv) Open source licenses do not restrict who can use the software or the fields of endeavor in which the software can be used. Therefore, OSS provides a net-centric licensing model that enables rapid provisioning of both known and unanticipated users.

(v) Since OSS typically does not have a per-seat licensing cost, it can provide a cost advantage in situations where many copies of the software may be required, and can mitigate risk of cost growth due to licensing in situations where the total number of users may not be known in advance.

(vi) By sharing the responsibility for maintenance of OSS with other users, the Department can benefit by reducing the total cost of ownership for software,

particularly compared with software for which the Department has sole responsibility for maintenance (*e.g.*, GOTS).

(vii) OSS is particularly suitable for rapid prototyping and experimentation, where the ability to "test drive" the software with minimal costs and administrative delays can be important.

(2) While these considerations may be relevant, they may not be the overriding aspects to any decision about software. Ultimately, the software that best meets the needs and mission of the Department should be used, regardless of whether the software is open source.

c. DoD Instruction 8500.2, "Information Assurance (IA) Implementation," (reference (g)) includes an Information Assurance Control, "DCPD-1 Public Domain Software Controls," which limits the use of "binary or machine-executable public domain software or other software products with limited or no warranty," on the grounds that these items are difficult or impossible to review, repair, or extend, given that the Government does not have access to the original source code and there is no owner who could make such repairs on behalf of the government. This control should not be interpreted as forbidding the use of OSS, as the source code is available for review, repair and extension by the government and its contractors.

d. The use of *any* software without appropriate maintenance and support presents an information assurance risk. Before approving the use of software (including OSS), system/program managers, and ultimately Designated Approving Authorities (DAAs), must ensure that the plan for software support (*e.g.*, commercial or Government program office support) is adequate for mission need.

e. There is a misconception that the Government is always obligated to distribute the source code of any modified OSS to the public, and therefore that OSS should not be integrated or modified for use in classified or other sensitive DoD systems. In contrast, many open source licenses permit the user to modify OSS *for internal use* without being obligated to distribute source code to the public. However, if the user chooses to distribute the modified OSS outside the user's organization (e.g., a Government user distributes the code outside the Government), then some OSS licenses (such as the GNU General Public License) do require distribution of the corresponding source code to the recipient of the software. For this reason, it is important to understand both the specifics of the open source license in question and how the Department intends to use and redistribute any DoD-modified OSS.

f. Software source code and associated design documents are "data" as defined by DoD Directive 8320.02 (reference (h)), and therefore shall be shared across the DoD as widely as possible to support mission needs. Open source licenses authorize widespread dissemination of the licensed software, thus allowing OSS to be shared widely across the entire Department. One way to make software source code accessible across the

Department is to use the collaborative software development environment at https://software.forge.mil/, operated by the Defense Information Systems Agency.

g. Software items, including code fixes and enhancements, developed for the Government should be released to the public (such as under an open source license) when all of the following conditions are met:

(1) The project manager, program manager, or other comparable official determines that it is in the Government's interest to do so, such as through the expectation of future enhancements by others.

(2) The Government has the rights to reproduce and release the item, and to authorize others to do so. For example, the Government has public release rights when the software is developed by Government personnel, when the Government receives "unlimited rights" in software developed by a contractor at Government expense, or when pre-existing OSS is modified by or for the Government.

(3) The public release of the item is not restricted by other law or regulation, such as the Export Administration Regulations or the International Traffic in Arms Regulation, and the item qualifies for Distribution Statement A, per DoD Directive 5230.24 (reference (i)).